FortiAuthenticator 3.1

What's New Guide

FortiAuthenticator 3.1 What's New Guide

June 16, 2014

Revision 1

Copyright© 2014 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard® are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Technical Documentation	http://help.fortinet.com
Knowledge Base	http://kb.fortinet.com
Forums	https://support.fortinet.com/forums
Customer Service & Support	https://support.fortinet.com
Training	http://training.fortinet.com
FortiGuard Threat Research & Response	http://www.fortiguard.com
License Agreement	http://www.fortinet.com/doc/legal/EULA.pdf
Document Feedback	Email: techdocs@fortinet.com

Table of contents

Change Log

Revision	Date	Change Description
1	2013-05-06	Initial Release.

Introduction

This document lists and describes many of the new features added to FortiAuthenticator 3.1. For a complete list of all new FortiAuthenticator 3.1 features, please see the latest release notes.

This document, and all of the FortiAuthenticator 3.1 documentation, will continue to improve as we see the new features in action and as we get feedback about these documents from you. You can send comments and suggestions for improvements for all FortiAuthenticator 3.1 documents to techdoc@fortinet.com.

What's New

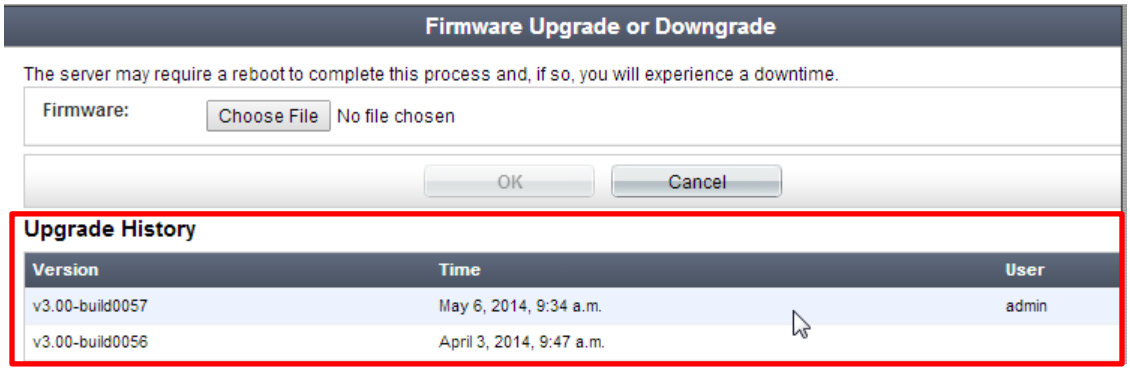
FortiAuthenticator 3.1 is a major feature release and includes new features in all functional areas of the product.

System features

These are features related to general system operation and not a specific functional area.

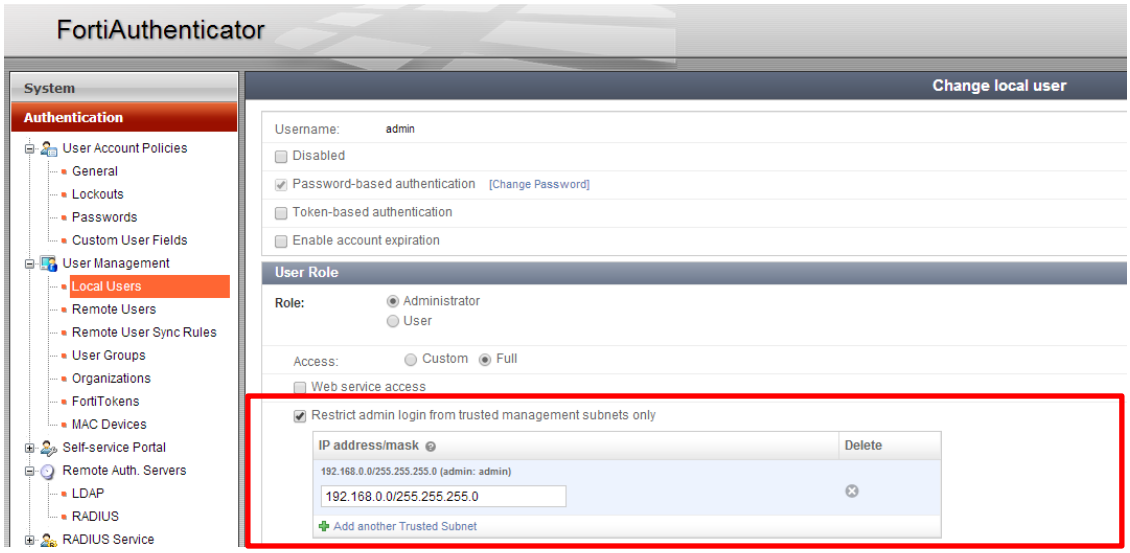
Upgrade History

The upgrade path taken to upgrade FortiAuthenticator to its current firmware is now captured in the GUI (for this release onwards). This is useful for support to identify incorrect upgrade paths which may cause stability issues.



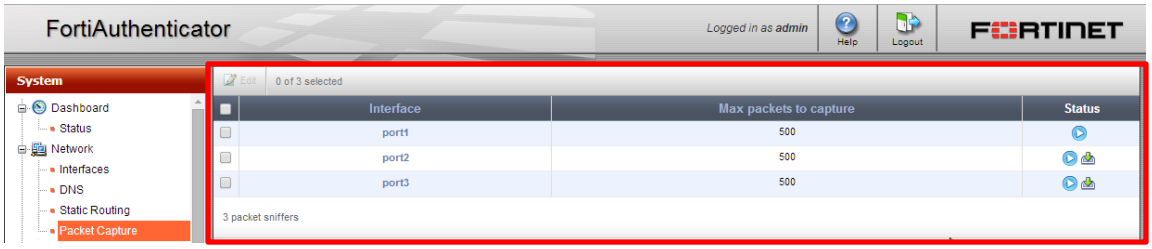
Admin GUI Access Control

To prevent unauthorized access to the admin GUI when the web interface is exposed, for example when the user portal is enabled, this release supports the ability to filter which subnets Administrative users can log in from e.g. a management subnet.



Packet Capture

Packet capture using the TCPDump utility is supported from the CLI. This release adds the ability to run the diagnostic utility from the GUI, on an interface to capture a specific number of packets. The resulting packet capture can be downloaded PCAP format for viewing directly in WireShark.

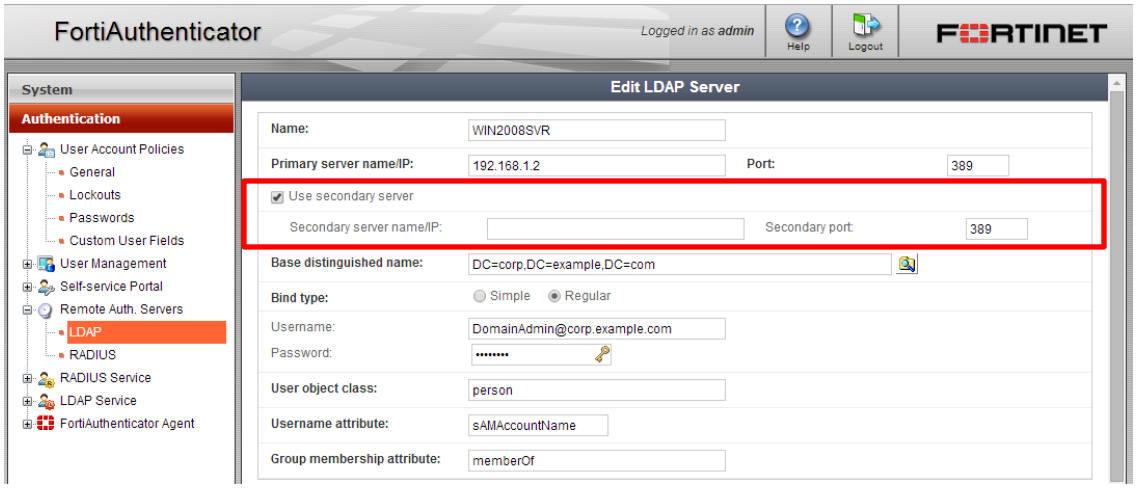


Authentication

Authentication covers all of the explicit authentication options within the FortiAuthenticator including RADIUS, LDAP, Two-Factor, Tokens, EAP, guest management and user self-service features.

Secondary LDAP server support

The previous limitation that only a single LDAP server could be configured for authentication purposes has been removed. A new option “Use secondary server” has been added to the LDAP Server configuration enabling high availability configuration.

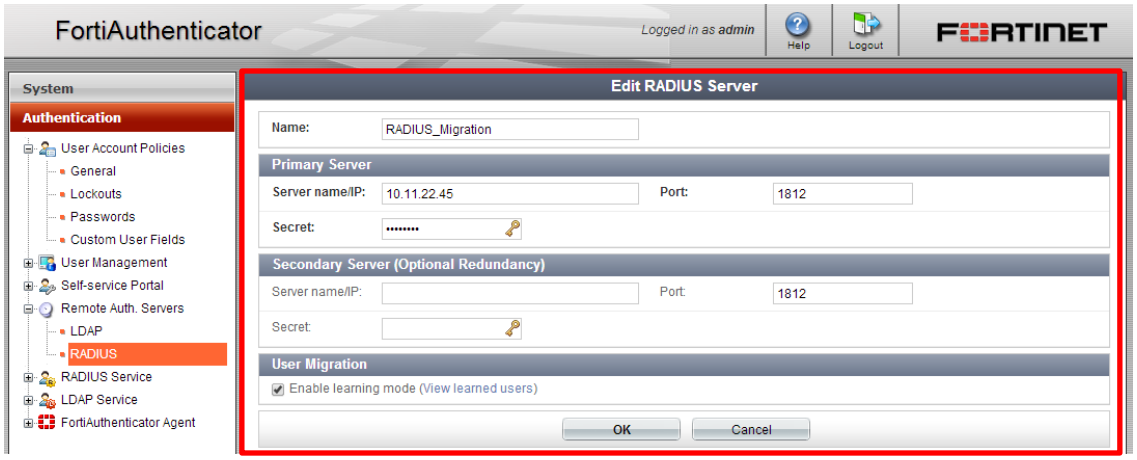


RADIUS Auth Server

FortiAuthenticator has supported proxying of authentication requests to an external LDAP server since its inception. This release introduces the ability to proxy authentication requests to external RADIUS Servers. This is a particularly useful feature when migrating away from competing third party two-factor authentication vendors.

When migrating, the users can retain their existing 2FA tokens and any RADIUS challenge-response requests will be proxied to the back end system. FortiAuthenticator also supports Learning Mode, whereby the user credentials will be automatically gathered and a new local user created using the users Username and Password (only supported for RADIUS clients using PAP). A list of learned users can be viewed via *Monitor* > *Learned RADIUS Users.*

Once the tokens expire, or the administrator is ready to migrate the users permanently, the user tokens can be replaced by FortiToken and the users migrated over to the FortiAuthenticator system, allowing the back end RADIUS system to be de-provisioned.

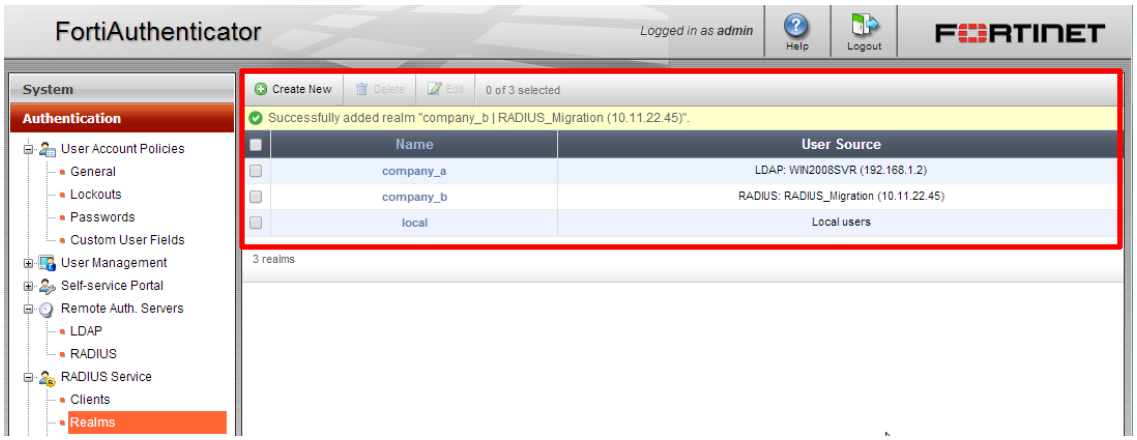


Auth to Multiple Realms

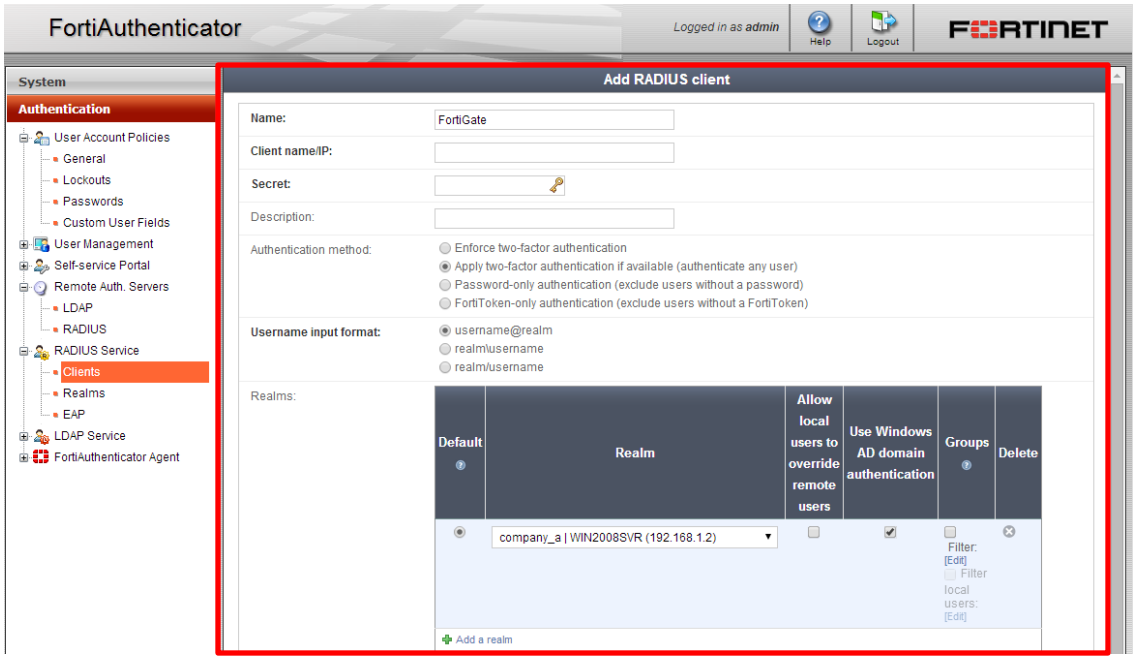
To support authentication in a multi-tenant environment, the concept of realms has been introduced. Each RADIUS realm is associated with a name e.g. domain or company name, which is used during the log in process to indicate which remote (or local) authentication server the user resides. The username of user john.doe belonging to Company_A would become:

- john.doe@company_a
- company_a\john.doe
- company_a/john.doe

depending on the format selected. FortiAuthenticator uses the specified realm to identify which back –end RADIUS or LDAP authentication server or servers to authenticate the user on.



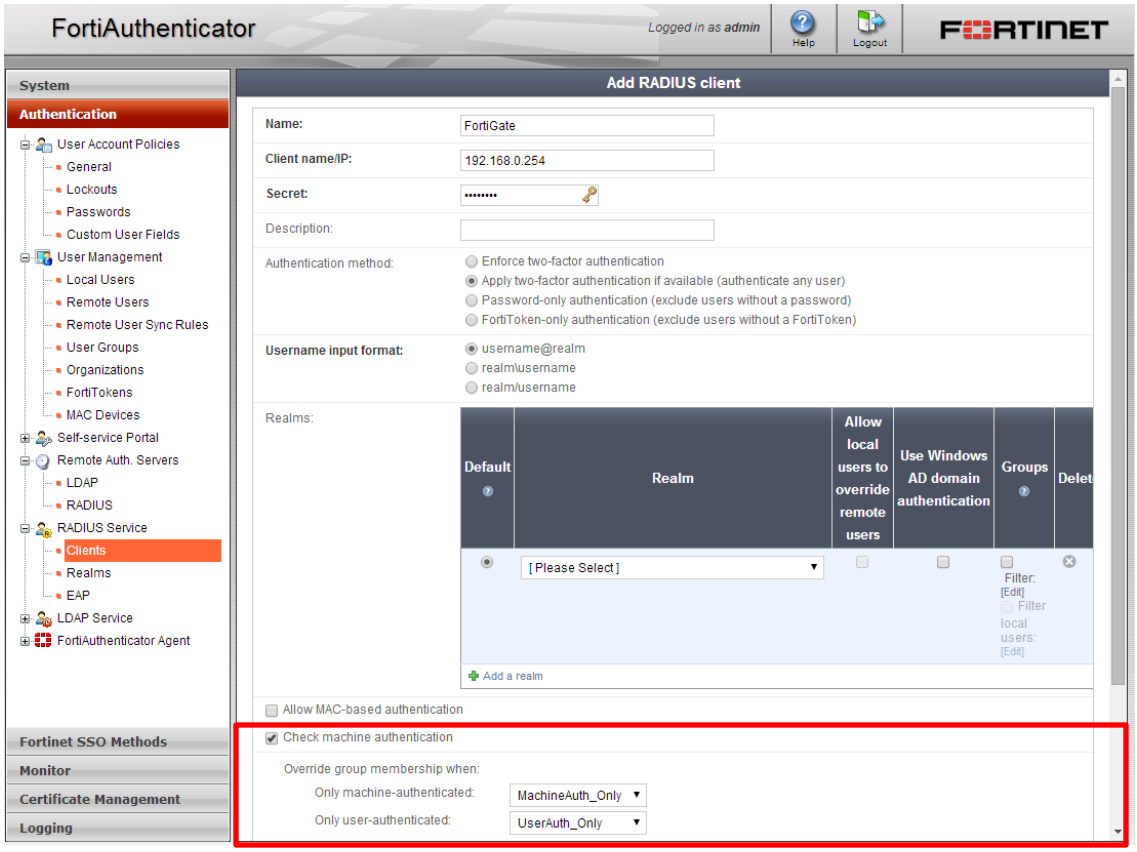
When configuring RADIUS Service clients, new settings allow acceptable realms to be configured on a per RADIUS Service Client (NAS) basis.



802.1X Machine Authentication

The ability to validate machine authentication for 802.1X authentications has been introduced in the release. Supporting Microsoft Windows Domain Authenticated systems and their native supplicants, this feature can be used to validate that the system connecting is authorized on the domain before granting access or to grant restricted access.

To achieve this, dummy groups are configured with specific RADIUS attributes to e.g. set Dynamic VLAN ID. These Groups do not need to contain any users,, they are just used to override the RADIUS Attributes for the connecting user. These dummy groups are applied to override the default RADIUS Attributes when the user is only Machine Authenticated or only user authenticated.

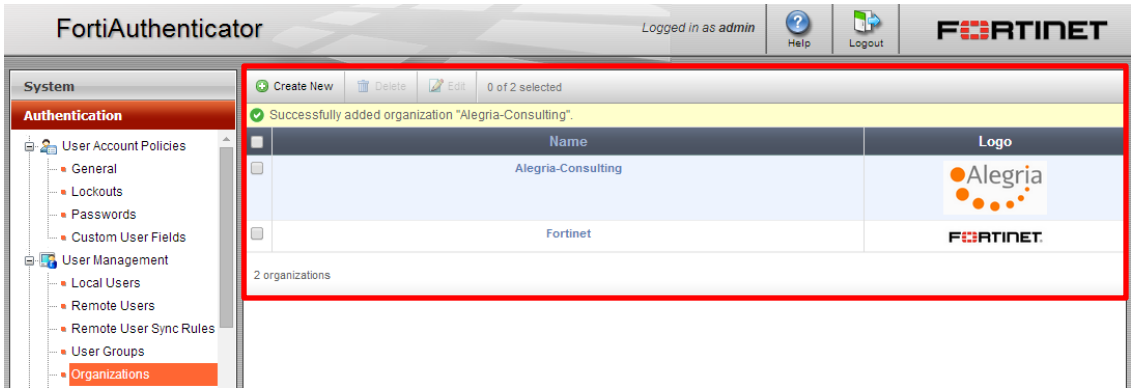


Machine Authentication commonly occurs on boot or on logout. Machine authentication does not occur for example when a device wakes from hibernation. For this reason, there is not always a recent machine authentication to rely on. For this reason, FortiAuthenticator caches authenticated devices, based on their MAC address, for a configurable period. Cached users can be found in *Monitor* > *Windows Device Logins*.

Support FTM Rebranding

FortiToken mobile (FTM) supports branding of the tokens stored within the application using a logo. Several new feature have been added to FortiAuthenticator to enable this.

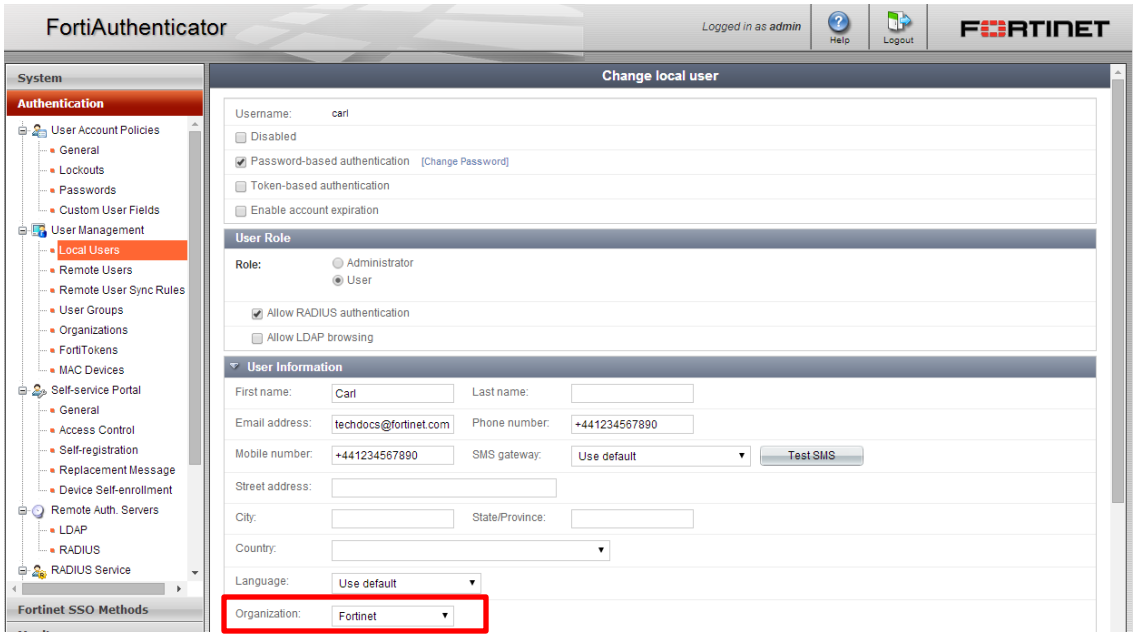
A new menu item Authentication > User Management > Organization has been created to allow an organization name to be mapped to its corresponding logo.



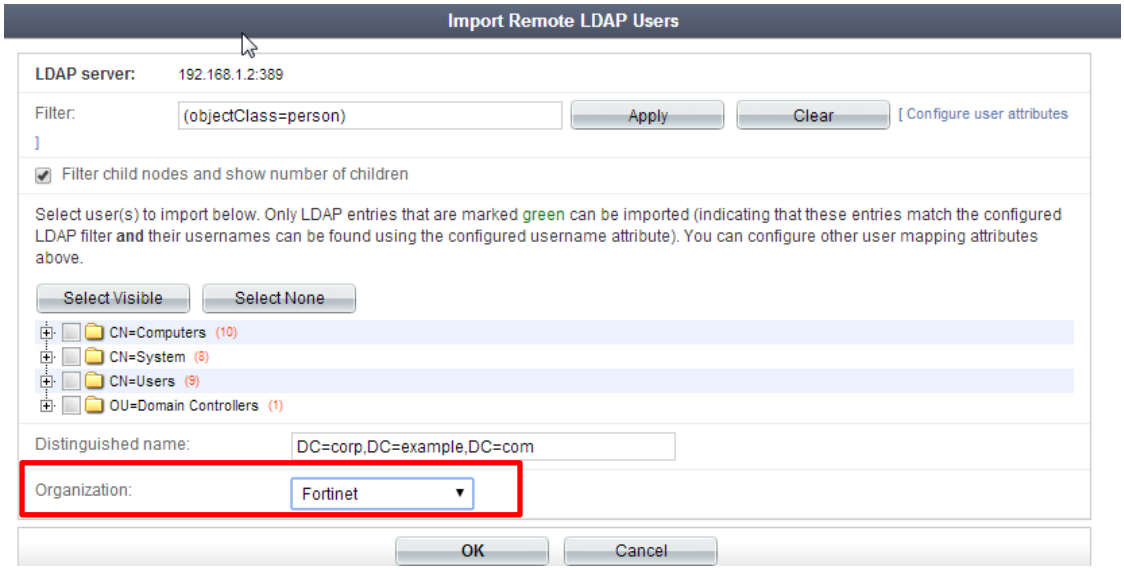
Logos should be a maximum of 320 x 320 pixels, 24 bit and in PNG format.

Once an organization has been created users can be assigned an affiliation in multiple ways.

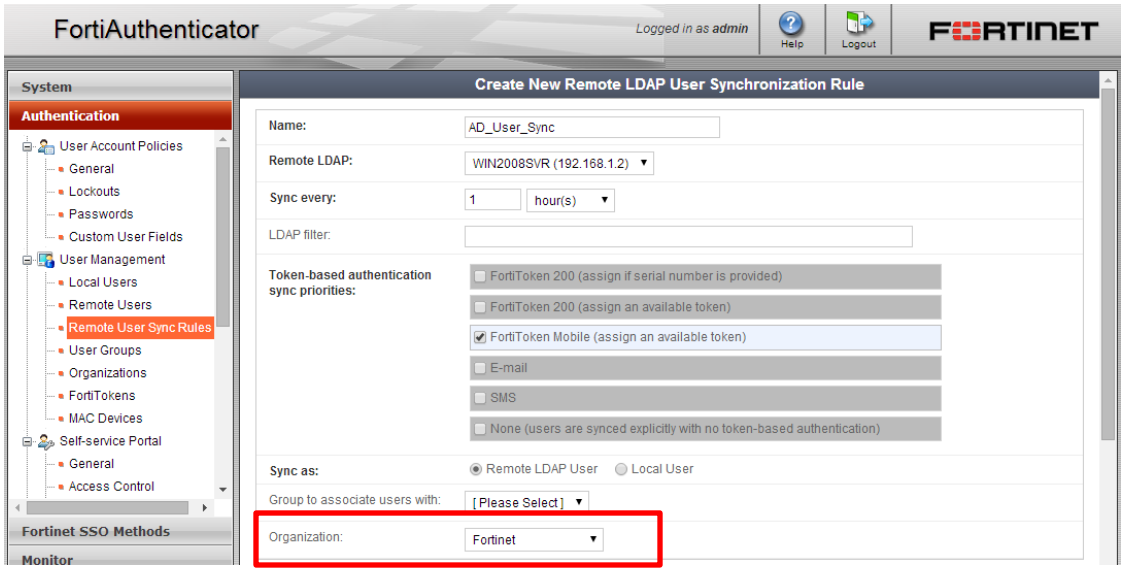
Local/Remote User Settings



Manual Remote User Import



Remote User Sync Rules



Once the Organization has been set for a user, the next provisioning of an FortiToken Mobile will utilize the Organization image during provisioning and the image will be pushed to the mobile device. Note that this is not done retrospectively for already provisioned tokens.

Customized Token

Fortinet Single Sign On

Fortinet Single Sign-On (FSSO) is a method used by FortiGate and FortiCache to transparently identify users on the network.

FortiAuthenticator uses both transparent and non-transparent methods to gather user login status information from a variety of disparate locations; consolidates and embellishes the information before supplying to FortiGate or FortiCache devices for use in identity based policies.

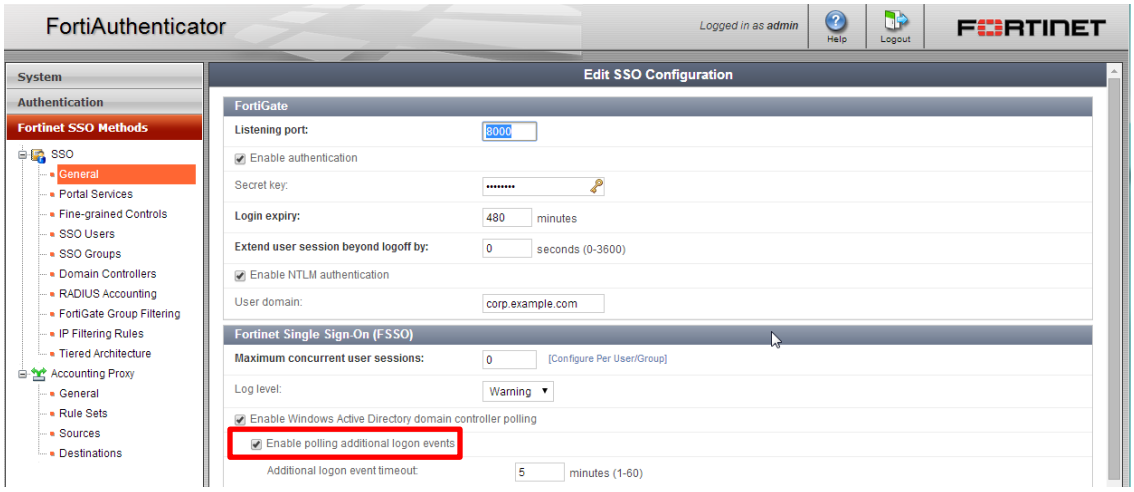
The previous methods of gathering user identity included:

FortiAuthenticator Portal Login	(Manual Login)
FortiAuthenticator Portal Login with home page widgets	(Partially transparent)
FortiAuthenticator Single Sign On Mobility Agent	(Transparent)
Active Directory Polling	(Transparent)
RADIUS Accounting	(Transparent)
DC Agent	(Transparent)
TS Agent	(Transparent)

FortiAuthenticator 3.1 introduces new FSSO functionality.

Enable polling additional logon events

FortiAuthenticator has added additional polling events which can be monitored as part of the Windows AD FSSO Polling feature. This is to capture events from additional systems such MacOSX and devices doing Kerberos authentication,



Standard Active Directory Logon Event IDs (Security event logs)

672

680

4776

4768

Additional Active Directory Logon Event IDs (Security event logs)

528

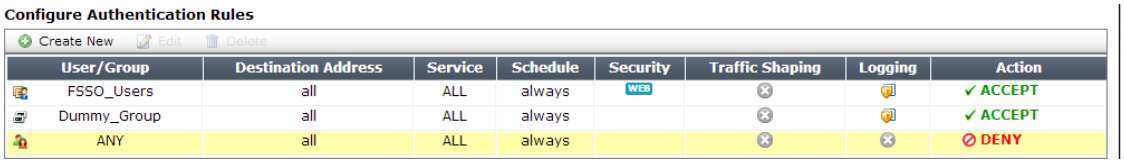
540

4624

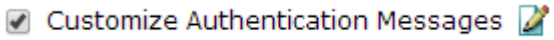
Redirect to original URL after auth

If a user is not authenticated, it is possible to use the last rule in a FortiGate Identity Based Policy to redirect a user to FortiAuthenticator for authentication. Previously, once the user authenticated e.g. using the captive portal, they would not be redirected to the originally requested URL. This release supports redirecting the user to their requested URL following successful authentication.

To enable redirect from the FortiGate to FortiAuthenticator, create an Identity Policy as shown below with a Dummy Firewall authentication rule as the second to last rule.



The reason this is a “Dummy” rule is because rather than authenticate the user, the page will be replaced with a redirect to the FortiAuthenticator. The create the redirect, Select Customize Authentication Messages and edit the code for the Login Page.



Replace the HTML code with the following (replacing <FAC_IP> with the IP address or URL of your FortiAuthenticator)

```
<html>
  <body>
    <script type="text/javascript">
      var URI_string = window.location.href;
      window.location.href = "http://<FAC_IP>/login/?next=" +
encodeURIComponent(URI_string);
    </script>
  </body>
</html>
```

When an unauthenticated user browses to e.g. www.google.com via the FortiGate, they will be redirected for FortiAuthenticator with the URL

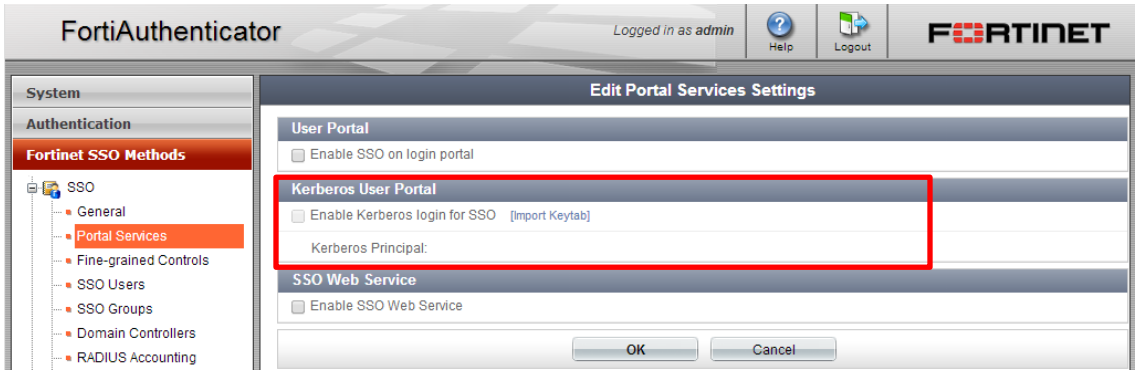
`http://<FAC_IP>/login/?next=http%3A%2F%2Fwww.google.com`

Following successful authentication, FortiAuthenticator will use the URL presented in the next variable to redirect the user to the originally requested content.

Kerberos based FSSO

The Kerberos authentication feature enables the FortiAuthenticator to identify the connecting user via a Kerberos exchange following a redirection from the FortiGate.

To configure the feature on FortiAuthenticator, enable the feature under *Fortinet SSO Methods > SSO > Portal Services*.



FortiAuthenticator requires a Keytab file describing your Kerberos infrastructure. To generate this file, you can use the Windows ktpass utility. The following code can be used in a batch file to simplify creation of the keytab file.

```
set OUTFILE=fac.keytab
set USERNAME=fac@corp.example.com

set PRINC=HTTP/fac.corp.example.com@CORP.EXAMPLE.COM
set CRYPTO=all

set PASSWD=Pa$$p0rt
set PTYPE=KRB5_NT_PRINCIPAL

ktpass -out %OUTFILE% -pass %PASSWD% -mapuser %USERNAME% -princ
%PRINC% -crypto %CRYPTO% -ptype %PTYPE%
```

In a similar way to the Redirect feature described above, the FortiGate can be configured to redirect unauthenticated users to the FortiAuthenticator, however the Kerberos authentication URL differs to the standard login URL. The Custom Message HTML for the Login Page HTML Redirect is as follows for Kerberos.

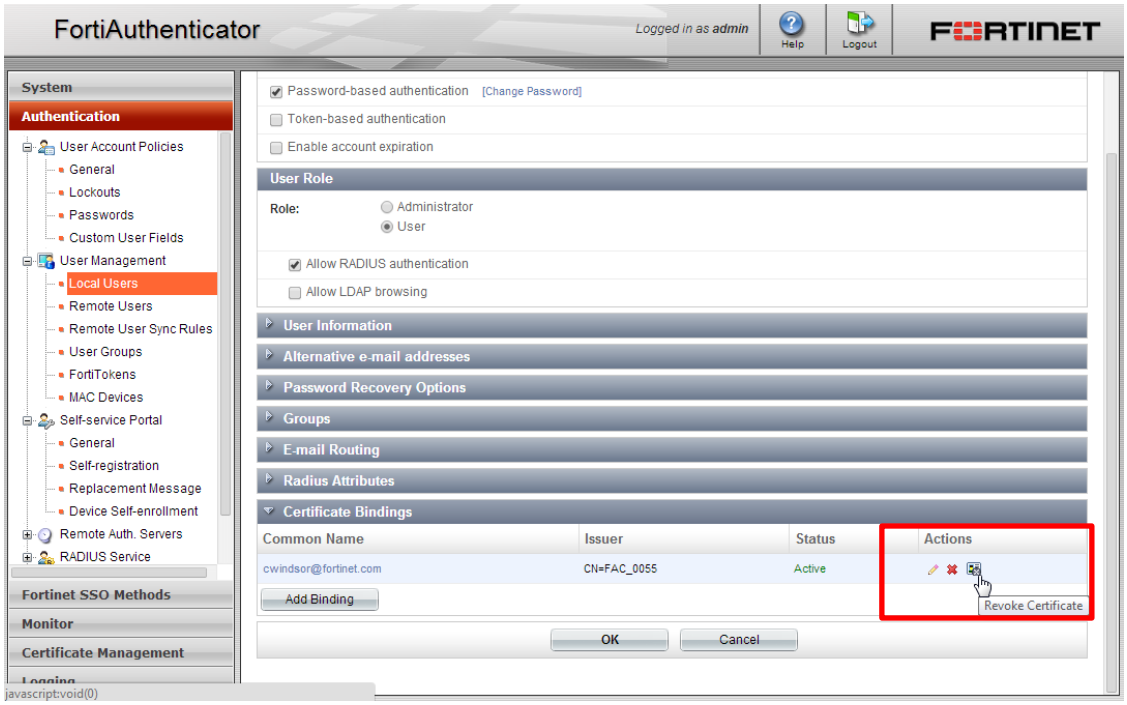
```
<html>
  <body>
    <script type="text/javascript">
      var URI_string = document.documentURI;
      document.location.href="http://<FAC_IP>/login/kerb-
auth?user_continue_url=" + encodeURIComponent(URI_string);
    </script>
    <h2>
      Redirecting.....
    </h2>
```

```
  </body>
</html>
```

Certificate Management

Improved user certificate revocation workflow

Previously, identifying a user's certificate and revoking was a multi-step process requiring several sections of the GUI, identifying the certificate *Common Name* and searching from the certificate list. This release adds the ability to revoke user certificates directly from the *Certificate Bindings* section of the *User* configuration.



API

Enable Token Provisioning

The FortiAuthenticator API has been extended to allow third party systems provision tokens and assign tokens to users. For more information see the FortiAuthenticator API Guide at http://docs.fortinet.com/fortiauthenticator/admin-guides/